REMARKS

The Examiner has maintained the rejection of the claims. As set forth below, such rejection is still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of at least one dependent claim into each of the independent claims. Since the subject matter of such dependent claim(s) was already considered by the Examiner, it is asserted that such claim amendments would **not** require new search and/or consideration.

The Examiner has rejected Claims 1-21, 24-32 and 41-43 under 35 U.S.C. 103(a) as being unpatentable over Coss et al. (U.S. Patent No. 6,098,172) in view of Minear et al. (U.S. Patent No. 5,983,350). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to at least substantially include the subject matter of former dependent Claims 5, 41, 42, and 43.

With respect to each of the independent claims, the Examiner has relied on the following excerpt from the Coss reference to make a prior art showing of applicant's claimed technique "wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field" (see this or similar, but not necessarily identical language in each of the independent claims).

> "...policy to use for a new network session. Each new session must be approved by the security policies of the source domain and the destination domain(s). For connections going to the Internet, it is likely that only a single domain check is performed. The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface. The incoming

> or outgoing network interface may be in the form of a network interface card (NIC), e.g., an Intel EtherExpress Pro 100B card available from Intel Corporation.
>
> FIGS. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required. In the firewall..." (Col. 6, lines 49-67)

The Coss reference teaches the approval of new network sessions by the security policies of source and destination domains, as well as packet processing by a firewall. However, unlike the Coss reference, applicant claims the identification of each port and service associated with the security policy "by an element identifier field, a field containing filter settings, and a log indicator field" (emphasis added). As a result, applicant's claims are distinct from the Coss reference.

Further, with respect to each of the independent claims, the Examiner has relied on the following excerpt from the Minear reference to make a prior art showing of applicant's claimed technique "wherein a security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field" (see this or similar, but not necessarily identical language in each of the independent claims).

> "8. A firewall, comprising:
>
> a first communications interface;
>
> a second communications interface;
>
> a first network protocol stack connected to the first communications interface, wherein the first network protocol stack includes an Internet Protocol (IP) layer and a transport layer;
>
> a second network protocol stack connected to the second communications interface, wherein the second network protocol stack includes an Internet Protocol (IP) layer and a transport layer;
>
> a security policy;

a decryption procedure, operating at the IP layer of the first network protocol stack, the decryption procedure receiving encrypted messages received by said first communications interface and outputting decrypted messages; and

an application layer proxy, connected to the transport layers of said first and second network protocol stacks, wherein the application layer proxy includes a plurality of authentication protocols, wherein each authentication protocol provides a different level of security, wherein the application layer proxy receives decrypted messages from the decryption procedure, selects an authentication protocol from the plurality of authentication protocols based on the content of the decrypted message, and executes the selected authentication protocol and wherein the application layer proxy determines based on the security policy whether the message is to be forwarded, and wherein the message is returned to the IP layer if the message is to be forwarded;

a third communications interface; and

a third network protocol stack connected to the third communications interface and to the application layer proxy, wherein the third network protocol stack includes an Internet Protocol (IP) layer and a transport layer and wherein the second and third network protocol stacks are restricted to first and second burbs, respectively." (Claim 8)

The above excerpt from the Minear reference teaches an application layer proxy that includes a plurality of authentication protocols. Applicant, on the other hand, teaches and claims "a security policy section of the policy file data structure [that] includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field" (emphasis added). Since no mention is made in the above excerpt regarding the use of any identifier fields, let alone those specifically claimed hereinabove, applicant's claims are clearly distinct.

Additionally, the Examiner has not even specifically addressed applicant's claimed technique "wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output

system) service;" "wherein a zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone;" "wherein a default zone is defined by addresses that are outside another zone;" and "wherein the security policy associated with the network protocol is specific to the network protocol." After careful review of both the Minear and Coss references, applicant notes that the above language claimed by applicant is clearly not even suggested by the prior art of record.

Furthermore, with respect to the independent claims, the Examiner has simply dismissed, under Official Notice, applicant's claimed techniques "wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document" and "wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged" under Official Notice.

Applicant notes that upon careful inspection of the prior art, neither the Coss nor the Minear reference mentions the storage of policy file data structures, much less policy file data structures stored as XML documents. Additionally, Applicant respectfully asserts that neither the Coss nor Minear references teach any sort of "default setting for a high security policy," and especially not in the foregoing detailed context claimed by applicant. Applicant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

> "If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to further distinguish applicant's claim language from the above reference, as follows:

> "wherein the zone is defined by a set of network addresses, which comprises at least one address outside the zone;
>
> wherein the network address dynamically assigned to the network adapter is determined by at least one of:
>
> mapping an adapter registry identifier to an associated network address stored in an operating system registry;
>
> monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address; and
>
> receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network" (see this or similar, but not necessarily identical language in each of the independent claims).

With respect to such subject matter of former Claim 5 (now at least substantially incorporated into each of the independent claims), the Examiner has relied on the following excerpt from the Coss reference, along with Claim 8 from the Minear reference (reproduced above), to make a prior art showing of such claimed feature.

> "701: the domain table is searched for a match of the interface name;
>
> 702: if a matching table entry is found, and if the IP address range is present in the matching table entry, the packet address is checked as to whether it is within the range; if so, the specified domain is selected; otherwise, the search continues with the next table entry;" (Col. 7, lines 61-67)

The Coss reference teaches a technique for searching a domain table for an interface name match and the comparison of a packet address to an IP address range. Further, the Minear reference teaches an application layer proxy that includes a plurality of authentication protocols. Nowhere in either of the references, however, is "[a] set of network addresses compris[ing] at least one address outside the zone" mentioned, as claimed by applicant (emphasis added).

With respect to the subject matter of former Claims 41, 42, and 43 (now at least substantially incorporated into each of the independent claims in Markush-type format), the Examiner has relied on the following excerpt from the Coss reference, along with Claim 8 from the Minear reference (reproduced above), to make a prior art showing of applicant's claimed technique "wherein the network address dynamically assigned to the network adapter is determined by mapping an adapter registry identifier to an associated network address stored in an operating system registry," "wherein the network address dynamically assigned to the network adapter is determined by monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address," and "wherein the network address dynamically assigned to the network adapter is determined by receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP

network" (see this or similar, but not necessarily identical language in each of the independent claims).

> "...example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions. A dynamic rule can be set for..." (Col. 9, lines 6-9)

The Coss reference teaches the loading of dynamic rules. The Minear reference teaches an application layer proxy that includes a plurality of authentication protocols. Applicant, on the other hand, claims the determination of the network address dynamically assigned to the network adapter "by mapping an adapter registry identifier to an associated network address stored in an operating system registry" (emphasis added). The prior art makes no mention of the determination of a network address, much less the determination by mapping an adapter registry identifier to an associated network address stored in an operating system registry.

Applicant also claims the determination of the network address dynamically assigned to the network adapter "by monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address" (emphasis added). The prior art makes no mention of the determination of the network address by monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic.

Additionally, applicant claims the determination of the network address dynamically assigned to the network adapter "by receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network" (emphasis added). After careful review of the above references, it is clear that no mention of applicant's specifically claimed technique is made in the prior art of record.

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

All of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P361/00.166.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100